FIVERITY

INSIGHTS FROM THE CYBER FRAUD NETWORK

2021 Synthetic Identity Fraud Report

October 2021

Table of Contents

SIF: An Emerging Threat

SIF 101

At its core, a synthetic identity fraud (SIF) profile is simply a fake persona comprised of a mix of identity elements (typically stolen from real people) like a name, social security number and address.

As a first step in helping banks standardize SIF reporting, the Federal Reserve developed this definition in April, 2021:

The use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.

While the definition is straightforward, the process used to develop SIF profiles is highly technical, involving the use of automation and machine learning.

syn·thet·ic
i·den·ti·ty fraud (n.)

The use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.

A Different Kind of Fraud

Although SIF bears some similarity to “traditional” identity theft, its development, behavior and impact is entirely unlike earlier generations of financial crime.

SCALABILITY

Bringing scale to fraudulent theft has made SIF one of the fastest-growing financial crimes.[1] Criminals use automation to scrape identity elements from the dark web and assemble millions of synthetic profiles.

EVASION

Criminals combine a detailed understanding of the U.S. payments system with sophisticated software to create profiles that are extremely difficult to detect.

Unlike traditional identity theft, there’s no victim that will notice a fraudulent charge and alert their bank.

VIRALITY

Once a SIF profile is able to establish a moderate amount of credit, it quickly opens five trade lines on average, typically at different banks.

By “piggybacking” additional SIF profiles to an account as authorized users, criminals are on their way to developing their next set of synthetic identities.

HARM

Global fraud rings and rogue states behind cyber fraud funnel proceeds into weapons proliferation, human trafficking and other serious crimes.

[1] McKinsey & Company (January 2019). “Fighting Back Against Synthetic Identity Fraud.”

The Road to SIF

Although SIF has likely existed in some form for decades, a mix of systemic issues and technological developments has spurred its tremendous growth.

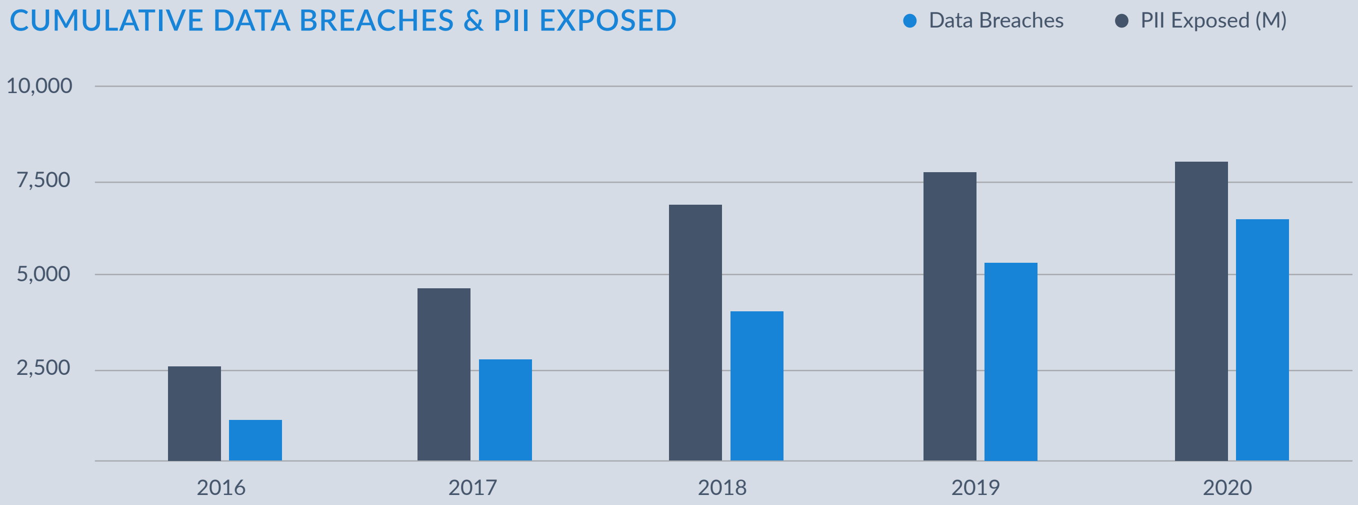
Reliance on SSNs

Social Security Numbers (SSNs) weren't created to catalogue U.S. citizens, so it's not surprising that they're an imperfect data source for identity verification. The Social Security Administration's move to randomized numbers in 2011 also removed a check between the first three digits and the applicant's state, making it easier for synthetic fraudsters to simply make up the number – which they do in 40% of loan applications.[2]

The expanded rollout of the electronic Consent Based SSN Verification (eCBSV) service in July 2021 has the potential to add some rigor to this identity element. Approved banks are now able to check an applicant's name, date of birth and SSN against this registry, but there are of course downsides. As a financial institution (FI) can't run checks on applicants outside of the U.S., one concern is that fraudsters will simply shift more operations abroad, or use VPNs to achieve this effect.[3]

Exposed PII

Although the amount of PII exposed each year has declined as hackers shift their focus from individuals to businesses, fraudsters have plenty to work with. In the past three years alone, a series of data breaches revealed 1.4 billion PII elements. The sheer amount of exposed data has turned PII into an affordable commodity. On the dark web, criminals can purchase a social security number for as little as $1, or a driver's license for $20.[4]



Cyber criminals can access billions of exposed identity elements on the dark web.

Identity Theft Resource Center (January 2021). 2020 in Review: Data Breach Report.

[2] ID Analytics (November 2019). "Slipping Through the Cracks: How Synthetic Identities are Beating Your Defenses."
[3] Joint Trades Letter to Social Security Administration Re: Agency Information Collection Activities (April 2021.)
[4] Experian (2019). "Here's How Much Your Personal Information is Selling for on the Dark Web."

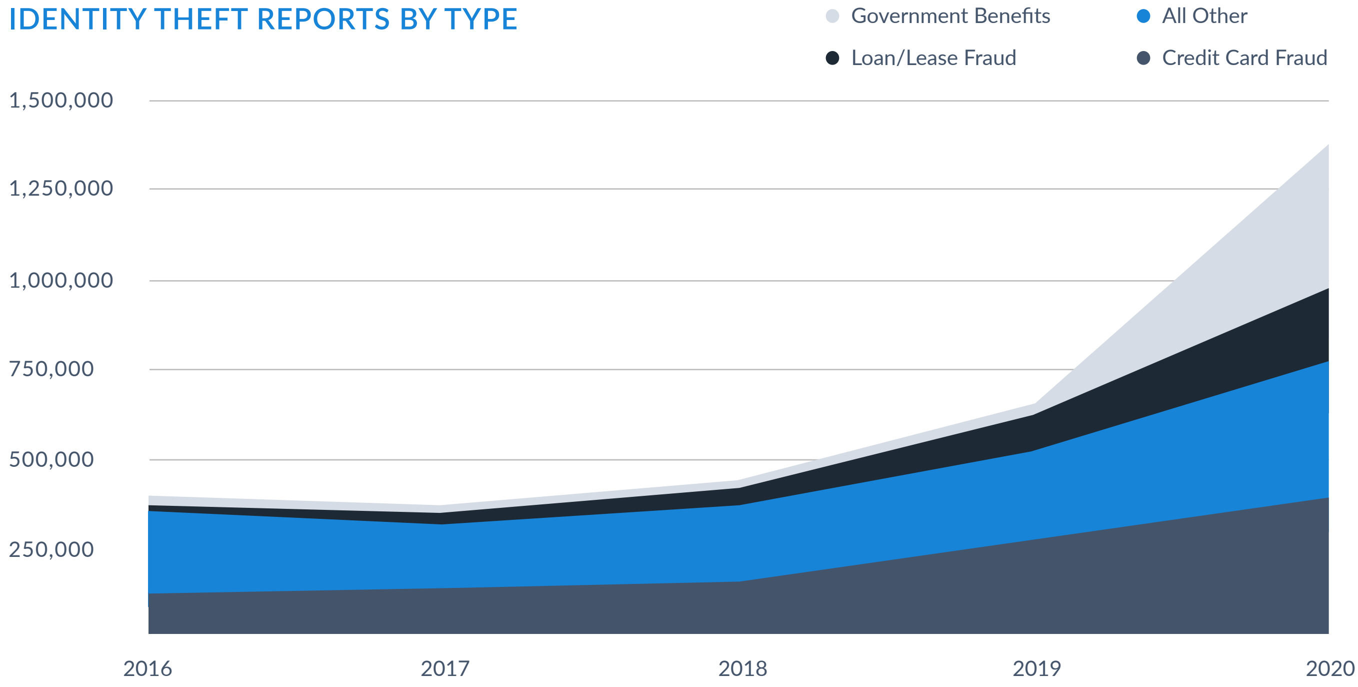
Pandemic-Driven Opportunities

In addition to the enormous human cost of the global pandemic, its impact on economic activity and online behavior has greatly accelerated the rise of cyber fraud.

Fraudsters Take Advantage

In response to the pandemic-driven economic downturn, the U.S. government developed safety net and stimulus programs to quickly help people in need. These programs were rolled out with a broad understanding that they'd be more susceptible to fraud than those with robust safeguards, and criminals took full advantage.

IDENTITY THEFT REPORTS BY TYPE



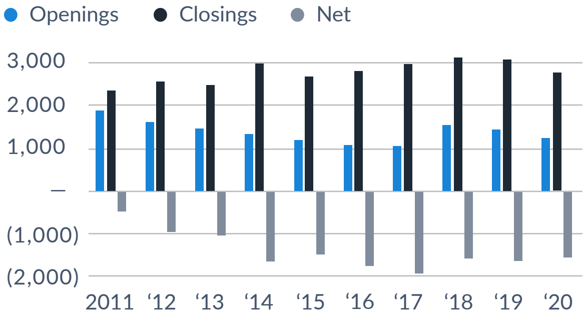
Government programs became a new and profitable target for cyber criminals during the pandemic.

FTC (Feb 2021). Consumer Sentinel Network Data Book 2020

Digital Transformation Accelerated

Covid-19 only accelerated a shift towards online banking that's been growing for years. The pandemic was especially successful at moving late adopters forward, with 90% of people over age 60 trying online banking for the first time.[5] This rise of online banking necessarily coincides with a decrease in analog banking, as the number of bank branches dropped by 14,824 over the past five years.[6]

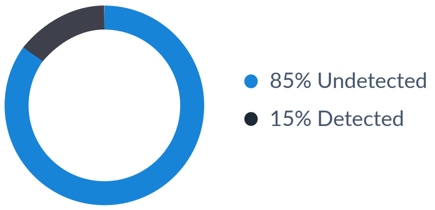
BRANCH OPENINGS & CLOSINGS



Source: Visual Capitalist

To accommodate this increase in online activity, FIs were forced to accelerate their digital transformation efforts. Fraud detection is arguably one area that lagged behind. Legacy identity verification systems that reliably caught traditional identity fraud were largely helpless in the face of new threats, missing 85-95% of likely SIF profiles.[7]

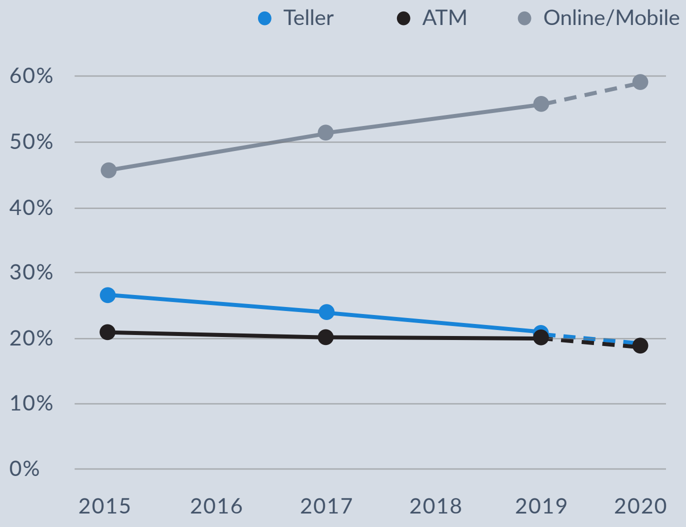
SIF DETECTION BY LEGACY ID VERIFICATION SYSTEMS



Source: ID Analytics

> With the pandemic hitting, banks had to quickly pivot in order to make services available for their customers. And in doing so, you don't necessarily have the time to put the proper controls in place. So, what the pandemic has done has potentially increased the magnitude for all types of fraud, with synthetic certainly being one of them.[8]
>
> Staci Shatsoff
> Associate VP, Payments Group
> Federal Reserve Bank of Boston

PRIMARY METHOD OF ACCESSING BANK ACCT



Late adopters helped move online banking ahead in 2020.

Source for 2015-2019: FDIC (2019). How America Banks: Household Use of Banking & Financial Services. 2020 estimate by FiVerity.

[5] Insider (May 2021). "US Digital Banking Users will Surpass 200 Million in 2022."
[6] Visual Capitalist (Feb 2021). "Why Branch Banking is Dying in America."
[7] ID Analytics (November 2019). "Slipping Through the Cracks: How Synthetic Identities are Beating Your Defenses."
[8] FiVerity (June 2021). Webinar: Defining the Synthetic Identity Fraud Threat.

Quantifying SIF's Impact

Challenges to Measuring SIF

Before getting into the size of the problem, it's worth exploring the difficulty of detecting – and therefore measuring – SIF.

STEALTH

Unlike ransomware, which requires the attention of the targeted company, SIF only succeeds when it's undetected. SIF flies below the radar by appearing similar to legitimate thin credit applicants, requesting small loans, and once approved, making payments on time. SIF accounts often maintain their secrecy even after busting out, as FIs attribute the theft to bad underwriting.

REPORTING

Aside from the obvious fact that banks can't report a crime they aren't aware of, guidelines for identifying and reporting SIF haven't been established. SIF is a relatively new crime, so there's no government database like the FTC's Sentinel in place to catalogue each incident.

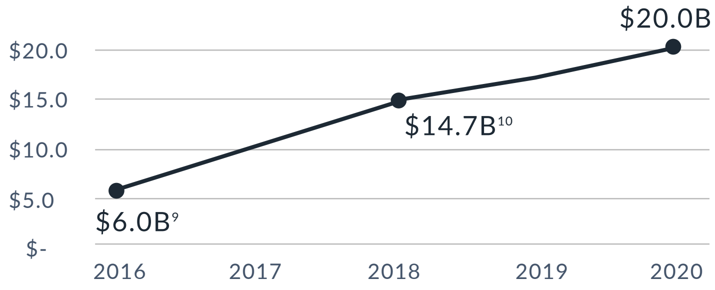
EVOLUTION

Using AI and machine learning, criminals have made SIF applications harder to detect over time. AI systems learn from approved and denied loan applications, which provide valuable input to the machine learning models. This feedback loop essentially helps the fraudsters identify the thresholds for each of the fraud detection rules used by legacy systems, and develop new profiles that are even better at evading them.

SIF's Growth

Synthetic identities represent a relatively small number of consumer accounts, but are responsible for a massive amount of theft. Insights from FiVerity's Cyber Fraud Network suggest SIF losses within U.S. FIs grew to $20 billion last year.

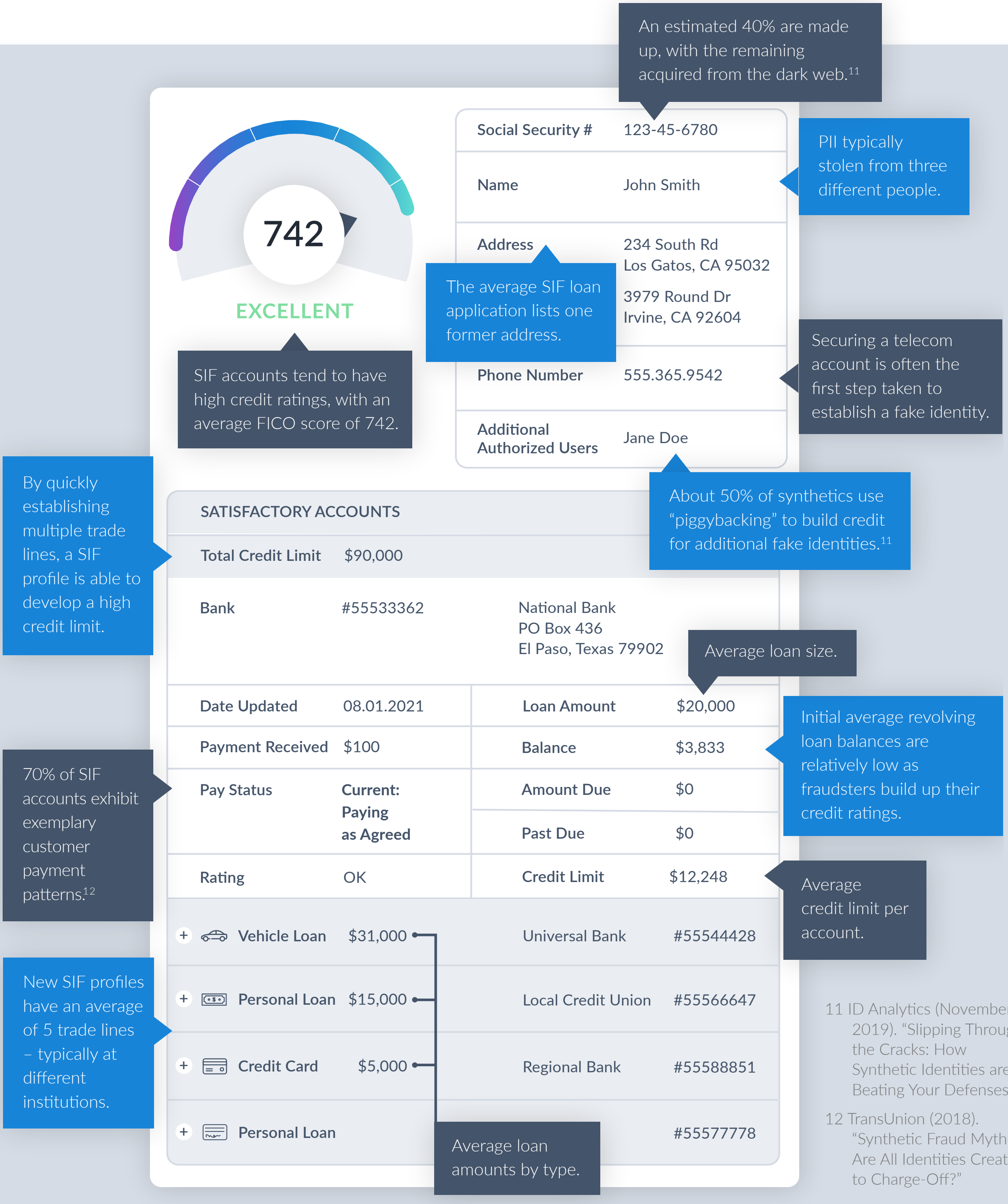
ANNUAL SIF LOSSES



[9] Auriemma Group (2018). "Synthetic Identity Fraud Cost Banks $6 Billion in 2016."
[10] Javelin Security & Research (2020).

Profile of a New SIF Account

FiVerity reviewed thousands of confirmed SIF accounts over the past three years to assemble the profile of a typical SIF account. These profiles start small, but over months (or years) they expand across multiple FIs with multiple trade lines, establishing a staggering amount of credit before busting out.



742

EXCELLENT

Social Security #	123-45-6780
Name	John Smith
Address	234 South Rd Los Gatos, CA 95032 3979 Round Dr Irvine, CA 92604
Phone Number	555.365.9542
Additional Authorized Users	Jane Doe

SATISFACTORY ACCOUNTS

Total Credit Limit $90,000

Bank	#55533362	National Bank PO Box 436 El Paso, Texas 79902	
Date Updated	08.01.2021	Loan Amount	$20,000
Payment Received	$100	Balance	$3,833
Pay Status	**Current: Paying as Agreed**	Amount Due	$0
		Past Due	$0
Rating	OK	Credit Limit	$12,248

+ Vehicle Loan	$31,000	Universal Bank	#55544428
+ Personal Loan	$15,000	Local Credit Union	#55566647
+ Credit Card	$5,000	Regional Bank	#55588851
+ Personal Loan			#55577778

An estimated 40% are made up, with the remaining acquired from the dark web.[11]

PII typically stolen from three different people.

The average SIF loan application lists one former address.

SIF accounts tend to have high credit ratings, with an average FICO score of 742.

Securing a telecom account is often the first step taken to establish a fake identity.

About 50% of synthetics use "piggybacking" to build credit for additional fake identities.[11]

By quickly establishing multiple trade lines, a SIF profile is able to develop a high credit limit.

Average loan size.

Initial average revolving loan balances are relatively low as fraudsters build up their credit ratings.

70% of SIF accounts exhibit exemplary customer payment patterns.[12]

Average credit limit per account.

New SIF profiles have an average of 5 trade lines – typically at different institutions.

Average loan amounts by type.

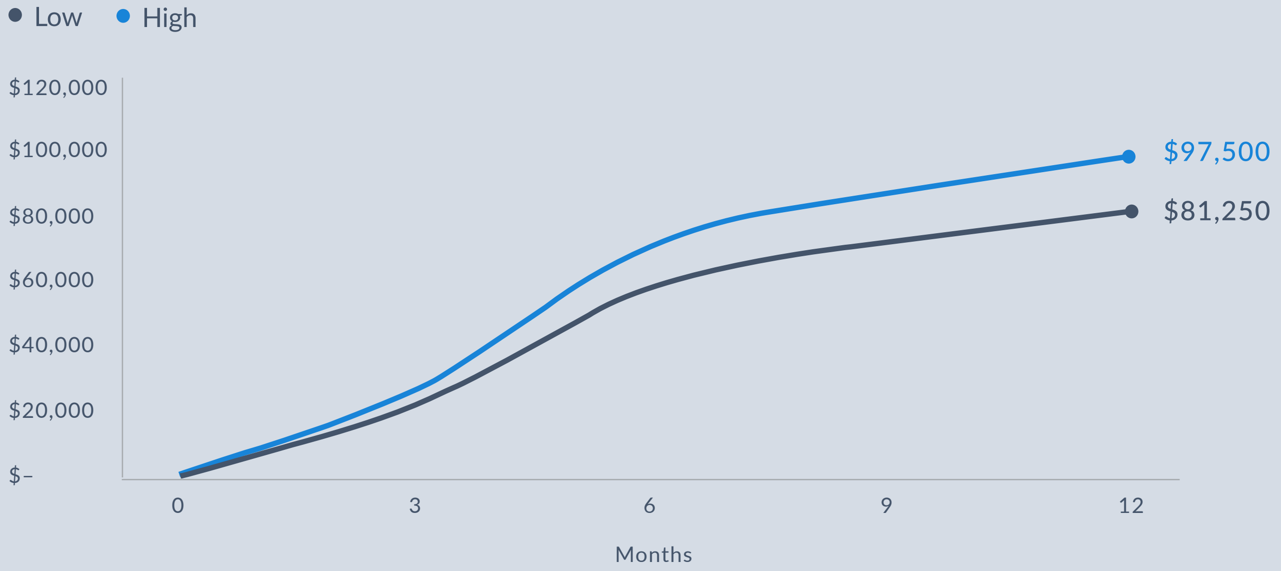
[11] ID Analytics (November 2019). "Slipping Through the Cracks: How Synthetic Identities are Beating Your Defenses."

[12] TransUnion (2018). "Synthetic Fraud Myths: Are All Identities Created to Charge-Off?"

Profile of a Mature SIF Account

The profile of an older SIF account is harder to determine. FIs that identify active SIF accounts naturally shut them down, and as noted earlier, thefts are often attributed to bad underwriting. FiVerity estimates the majority of SIF bust outs represent an increase of 25% to 50% above the credit limit obtained shortly after opening, for an average theft of $90,000. This amount doesn't include the fraudsters' occasional tactic of claiming to be the victim of identity theft in order to double their take.

BUST OUT RANGE



Across multiple trade lines, new SIF profiles obtain $65K in less than six months. A successful bust out typically ranges from $81K to $98K.

FiVerity estimates the average bust-out amount per SIF profile is **$90,000**

Fighting Back

Machine Learning

Cyber fraudsters are harnessing the power of automation and machine learning to create tens of thousands of accounts that effectively bypass legacy fraud detection systems. These legacy systems start with a “top down” picture of what a fraudulent application looks like, driven by static rules that indicate suspicious activity – like a high volume of credit inquiries or multiple addresses over a short time period. The more boxes that are checked, the higher the fraud score. By applying machine learning to approved and rejected applications, fraudsters create increasingly effective profiles.

Needless to say, banks can use the same technology to identify these attacks. Artificial intelligence approaches like machine learning turn things upside down...literally. Instead of assuming what a fraudulent account looks like, machine learning takes a “bottom up” approach, searching profiles for patterns that match those of recently confirmed fraudsters. Instead of checking against a set of static rules, machine learning systems determine what the fraudsters are up to as their tactics evolve.

Interbank Collaboration

Due to the viral nature of a SIF profile – which typically infects five to ten banks – sharing information across FIs is especially effective. While banks have been aiming to collaborate in fighting fraud for many years, a range of legal, competitive and logistical concerns have held these efforts back – most notably, restrictions on sharing consumer PII. Modern data encryption and other technologies however, offer the potential to facilitate widespread intelligence sharing while meeting the customer privacy and other needs of FIs.

Distributed encryption across a broad network ensures that no single institution holds the complete key to decrypt consumer data. In this case, each company within the network can access a fraudulent profile only if they’re already in possession of the corresponding PII. This allows companies to receive alerts on fraudsters that have accounts within their portfolio but prevents them from seeing additional information on their competitors’ customers.

> No single organization can stop wide-ranging, fast-growing synthetic identity fraud on its own. Fraudster tactics continually evolve to stay a step ahead of detection – and the most sophisticated fraudsters can operate at scale in organized crime rings, generating significant losses for the payments industry. It is imperative that payments industry stakeholders work together to keep up with the evolving threat posed by synthetic identity fraud, which includes anticipating future fraud approaches.[13]
>
> The Federal Reserve

[13] The Federal Reserve (Oct 2019). Payments Fraud Insights: Detecting Synthetic Identity Fraud

Intrabank Collaboration

In addition to collaboration across banks, silos between fraud detection and cybersecurity teams *within* banks can be removed to improve fraud detection. These teams historically focused on different threats from different types of criminals, so collaboration wasn't a priority. By merging elements of identity theft with cyber attacks however, criminals are taking advantage of the gap between these departments.

An effective partnership between these teams goes beyond information sharing, however. It requires both departments to get educated on the criminal organizations and individual hackers working against them, combine defensive playbooks, jointly evaluate new technologies, and coordinate reporting with law enforcement.

A positive development within some banks has been the creation of "cyber fusion" centers, which brings cybersecurity and fraud analysts together to create a holistic view of shared threats.

Fighting Fire with Fire

SIF accounts are extremely hard to detect at the initial loan application stage, and even harder to identify once they become customers that make on-time payments. From the technology used to develop profiles to its patient approach to theft, SIF is successfully taking advantage of the industry's legacy approach to fraud detection.

Taking a page from the fraudsters' technique by adopting machine learning has proven to be the most effective way of uncovering this evolving threat. Once a fraudster has been exposed, *securely* sharing this information with other FIs is a low-cost and impactful way to stop its spread.

While there isn't a silver bullet to tackling SIF, or any other type of cyber fraud, the industry needs to modernize its efforts to identify and stop these attacks before they gain a foothold into the payments system.

Once a fraudster has been exposed, *securely* sharing this information with other FIs is a low-cost and impactful way to stop its spread.

FIVERITY

FiVerity provides financial institutions with cyber fraud defense to combat a dangerous and growing threat - the convergence of fraud-related theft with sophisticated cyber attacks. Unlike traditional forms of fraud, emerging crimes like synthetic identity fraud (SIF) are perpetuated by global criminal organizations with significant resources and engineering skill. FiVerity leverages machine learning to identify these evolving threats, increasing an institution's fraud detection rates by over 50%.

FiVerity's Cyber Fraud Network further strengthens each user's defense by responding to fraudulent activity detected through the company's partnerships with banks, credit unions, regulators and law enforcement agencies. This multiplies each user's ability to identify – and learn from – new fraud patterns. In addition to ongoing defense, FiVerity offers a fast and lightweight portfolio analysis to identify SIF accounts and other forms of fraud within existing portfolios.

Visit fiverity.com to learn more